



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/001,431	10/31/2001	George S. Gales	10016933-1	2381

7590 01/19/2006

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER

PERUNGAVOOR, VENKATANARAY

ART UNIT PAPER NUMBER

2132

DATE MAILED: 01/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

MAILED

Application Number: 10/001,431
Filing Date: October 31, 2001
Appellant(s): GALES ET AL.

JAN 19 2006

Technology Center 2100

James L. Baudino
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 12/27/2005 appealing from the Office action mailed 8/31/2005.

(1) Real Party in Interest

The present application is assigned to Hewlett-Packard Development Company, L.P.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6279113 B1

Vaidya

8-2001

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

(a) Claims 1 and 3-29 are rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent Publication No. 2002/0116639 A1 to Chefalas et al.

(b) Claims 2 is rejected under 35 U.S.C § 103(a) as being unpatentable over Chefalas in view of U.S. Patent No. 6,279,113 B1 to Vaidya

(10) Response to Argument

(a) Appellant's arguments regarding Claim 1-11 are not persuasive. As Chefalas discloses the VDL file being human-readable and machine-readable see Par. 0044 & Par. 005. As Chefalas mentions the routing of data packet using the business event which is contained within aforementioned data packet, which clearly means it is machine-readable. And further, as it is commonly known in the art that transmission of data packets for routing from server to client is machine-readable further exemplified in Par. 0045. And the Appellant's arguments regarding the file being human-readable is also not persuasive. As Chefalas discloses the manager being paged about the virus and further of logging of the client see Par. 0046. And further, Chefalas also mentions the user interface about the virus and the repair/removal of the file see Par. 005-006. As also the Chefalas mentions the communication between client and server in Par. 0045, which is suggestive of human-readable virus checking process. And further the business event being used by the system administrator for analysis see Par. 0059 thus

further buttressing the Examiner's claim the VDL file is human-readable. And further Chefalas mentions the indexing of entries within the file see Par. 0046, which is clearly indicates business events listed in a file.

And the Appellant's argument's regarding Claim 1 not containing "at least one attribute of the specified attack" is not persuasive. As Chefalas discloses the types of viruses being listed and further the appropriate action to be taken based on the severity of virus see Fig. 5A, as it is apparent the Chefalas recognizes that virus A is less severe than virus F, which disconnects the client as opposed to virus A which merely logs action.

(b) Appellant's arguments regarding Claim 12-16 are not persuasive. As Chefalas discloses the human-readable and machine-readable file see part (a) for rejection.

And further the Appellant's arguments regarding Chefalas not disclosing "at least one attribute of the specified attack and the severity of the specified attack" is not persuasive. As Chefalas mentions the responding based on type of virus(virus name/computer that emanated from) see Fig. 5A-5B, which ranges from merely logging action to disabling router and client. And further, Chefalas is suggestive of the computing platform of the system see Par. 0041-0042, as Chefalas discloses the making distinction between PDA and notebook computer. And more succinctly in Par. 0039 where Chefalas discloses the Windows operating system and Java based programs(i.e. Mac OS).

(c) Appellant's arguments regarding Claim 17-29 are not persuasive. As Chefalas discloses the human-readable and machine-readable file see part (a) for the rejection.

And further the Appellant's arguments regarding Chefalas not disclosing "interpreter" is not persuasive. As Chefalas discloses the identifying the virus that the related policy see Fig. 5A. And further, Chefalas discloses the comparing of event to policy see Fig. 8 item 802, thus suggesting of parsing the attack and policy in the file. And further the Appellant's arguments regarding "pursuant to a predetermined format" is not persuasive as Chefalas discloses the organization of data packets in a predetermined format see Fig. 4A-4B(where the virus name is first, then action taken, then computer id and so on) and further the header and payload see Par. 0044. And further Chefalas discloses that the policy may be arranged in any data structures possible see Par. 0048.

For an more thorough treatment of all of the rejections please consult the Final Rejection herein enclosed.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

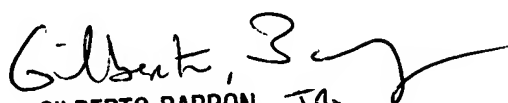
Respectfully submitted,

Venkat Perungavoor

Venkat Perungavoor

Art Unit 2132

Conferees:


GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Gilberto Barron Jr

Justin Darrow

Appendix

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed 8/12/2005 have been fully considered but they are not persuasive. As Chefalas et al.(hereinafter Chefalas) in U.S. Patent Publication No. 2002/011639 A1 discloses the file for which a generating a log and further an VDL file that identifies a attack, one attribute of specified attack, a policy definition and an least attribute of the attack see Fig. 4A-5B & Par. 0046.
2. For citation of 35 USC § 102(e) and 35 USC § 103(a) please consult previous office action.

Response to Amendment

Claim Rejections - 35 USC § 102

3. Claim 1, 3-29 rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Publication No 2002/011639 A1 to Chefalas et al.(hereinafter Chefalas)
4. Regarding Claim 1, Chefalas discloses generating a log file and a file that contains instructions for viruses see Fig. 4A-5B & Par. 0046; specifying the name of virus being detected (identity of an attack) and what computer it was detected(an attribute of attack) on see Par. 0030. Further, Chefalas discloses specifying an policy with regard to the virus(policy definition with respect to attack) and also discloses an attribute of the policy see Par. 0030 & Par. 0044 & Par. 0060.

5. Regarding Claim 3, 13, Chefalas discloses the specifying security category of the specified attack and further discloses the policy with respect to specified category see Figure 5A.
6. Regarding Claim 4, Chefalas discloses the security product executing on the computer system see Par. 0012.
7. Regarding Claim 5, Chefalas discloses the identification of the severity associated with a breach see Par. 0044.
8. Regarding Claim 6, Chefalas discloses the type of virus that infected the client(specifying description of the attack) see Par. 0060.
9. Regarding Claim 7, Chefalas discloses the specifying of why the specified attack is important and the need for protection see Par. 0059.
10. Regarding Claim 8, 14, Chefalas discloses the reporting of information to a manager(specifying how information is reported to a user with respect to an specified attack) see Par. 0030 & 0047.

11. Regarding Claim 9, 15 and 16, Chefalas discloses scheduling of maintenance of server in response to breach and further to repair the vulnerability (specifying an application operable to respond to breach) see Par. 0060.

12. Regarding Claim 10, Chefalas discloses the specifying network protocols, data patterns and action in response to detecting specified network protocol and data pattern see Par. 0054-0058.

13. Regarding Claim 11, Chefalas discloses the what action to take in response to an attack (specifying a direction of data flow) see Par. 0062.

14. Regarding Claim 12, Chefalas discloses generating a log file and a file that contains instructions for viruses see Fig. 4A-5B & Par. 0046; specifying the name of virus being detected (identity of an attack) and what computer it was detected and type (an attribute of attack) on see Par. 0030. Further, Chefalas discloses specifying an policy with regard to the virus (policy definition with respect to attack) and also discloses an attribute of the policy see Par. 0030 & Par. 0044 & Par. 0060. And further the computing platform of the system see Par. 0033.

15. Regarding Claim 17, Chefalas discloses generating a log file and a file that contains instructions for viruses see Fig. 4A-5B & Par. 0046; an vulnerability description file containing definition of attack and policy item for the attack see

Figure 4A items 406 & 408, an interpreter to parse the attack and policy and organize to an predetermined format see Par 0046-0048; an data storage to store parsed and organized information accessible by an application see 0048.

16. Regarding Claim 18, Chefalas discloses the use of relational database see Par. 0048.

17. Regarding Claim 19, Chefalas discloses the use of memory for data storage see Par. 0040.

18. Regarding Claim 20, Chefalas discloses the definition of a security product see Par. 0047.

19. Regarding Claim 21, Chefalas discloses the grouping of one attack and an policy see Fig. 5A.

20. Regarding Claim 22, Chefalas discloses the definition of an computing platform see Par. 0033.

21. Regarding Claim 23 and 25, Chefalas discloses the type of attack and which client was infected and time it was infected see Par. 0060 & Fig. 5A.

22. Regarding Claim 24, Chefalas discloses the identification of the severity associated with a breach see Par. 0044.

23. Regarding Claim 26, Chefalas discloses the displaying and reporting of results of the attack see Par. 0047.

24. Regarding Claim 27, Chefalas discloses scheduling of maintenance of server in response to breach and further to repair the vulnerability(specifying an application operable to respond to breach) see Par. 0060.

25. Regarding Claim 28, Chefalas discloses the specifying network protocols, data patterns and action in response to detecting specified network protocol and data pattern see Par. 0054-0058.

26. Regarding Claim 29, Chefalas discloses the what action to take in response to an attack(specifying a direction of data flow) see Par. 0062.

Claim Rejections - 35 USC § 103

27. Claim 2 rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Publication No 2002/011639 A1 to Chefalas et al.(hereinafter Chefalas) in view of U.S. Patent 6279113 B1 to Vaidya.

28. Regarding Claim 2, Chefalas discloses the specifying of computing platform of the computing system see Par. 0033. But Chefalas does not disclose the signature of the attack. However, Vaidya discloses the signature of the attack see Abstract & Col 2 Line 30-52. It would be obvious to one having ordinary skill in the art at the time of the invention to include signature of attack of Vaidya's in the invention of Chefalas in order to catalog specific signatures as taught in Vaidya see Col 2 Line 34-36.

Conclusion

29. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

30. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Venkatanarayanan Perungavoor whose telephone number is 571-272-7213. The examiner can normally be reached on 8-4:30. If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

31. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Venkatanarayanan Perungavoor
Examiner
Art Unit 2132

8/24/2005

Justin Darrow
JUSTIN T. DARROW
PRIMARY EXAMINER